

A California Business Privacy Handbook



California Office of Privacy Protection
Department of Consumer Affairs

July 2006

This brochure is for informational purposes and should not be construed as legal advice or as policy of the State of California. If you want advice in a particular case, you should consult an attorney-at-law or other expert. The brochure may be copied, if (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the Office of Privacy Protection in the California Department of Consumer Affairs, and (3) all copies are distributed free of charge.



California Office of Privacy Protection
Department of Consumer Affairs
www.privacy.ca.gov
866-785-9663

A California Business Privacy Handbook

The ABCs of Protecting Personal Information and Helping to Prevent Identity Theft

Business can play an important role in protecting privacy and curbing the growth of identity theft. The purpose of this Handbook is to give California businesses a simple guide to basic practices for handling personal information responsibly. For most practices, we cite a relevant California or federal law.

The California Office of Privacy Protection

The California Office of Privacy Protection, in the California Department of Consumer Affairs, was created out of the growing concern about individual privacy and identity theft. The Office's responsibilities include helping identity theft victims and others with privacy questions and making recommendations of practices that protect individual privacy.

Fastest Growing Crime

In recent years, identity theft has become the fastest growing crime in the nation. Over 9 million people – including more than a million Californians – became victims of identity theft in 2004. This terrible crime can cost victims hundreds of dollars and hundreds of hours to clear up. And it costs American business billions: \$52.6 billion in 2004, according to the Better Business Bureau.

Law enforcement explains the alarming growth in identity theft – up by as much as 80% in 2002 – by the relative ease of committing the crime. It's often far too easy for dishonest people to get access to other people's personal information, information like Social Security number, driver's license number,

credit card numbers, and other financial account numbers. Using one or more of these numbers, an identity thief can charge items to someone else's credit card, use someone's bank account, open a new charge account or bank account, and even buy a car or a house in some else's name.

While the victim may not always be liable for debts fraudulently run up in his or her name, clearing up records can be a lengthy and costly process. And the financial institutions or retailers involved are stuck with the charges!

Keeping Up with New Laws

Law makers have responded by passing laws to help identity theft victims and to require businesses to protect the security and confidentiality of their customers' and employees' personal information. California has been a national leader in identity theft prevention and remediation laws. This Handbook can help you keep up with many privacy laws and best practices. It is not intended as legal advice or as a comprehensive guide to privacy laws or information-handling practices. See the Resources section at the end for additional information.

A is for Access to personal information.

Controlling access to the personal information in your care is essential to preventing identity theft.

DON'T

- Leave documents containing sensitive personal information—such as Social Security numbers, driver's license numbers, financial account numbers, or medical information—lying out where anyone can see them.
- Use faxes, email or voice mail to send messages containing sensitive personal information.

DO

- Limit your employees' access to personal information to just what is necessary for them to perform their duties.
- Require employees to use passwords for access to databases containing personal information. This will provide an "audit trail" to track any abuses that may occur.
- Adopt a "clean desk policy" of keeping records containing sensitive personal information that are not being used in locked drawers or cabinets.
- Train your employees in their responsibilities for protecting personal information from unauthorized access.
- Use generally accepted security practices to protect sensitive personal information. See the Resources section at the end of this brochure.

B is for Breach of security.

DO

- Protect personal information from being accessed or acquired by unauthorized persons.
- Notify individuals in writing if certain items of their personal information are acquired by unauthorized persons. The types of information that trigger the notice requirement are name plus any of the following:
 - Social Security number
 - Driver's license number or California identification card number
 - Financial account number, along with any required PIN or password.

- Read the California Office of Privacy Protection’s “Recommended Practices on Notification of Security Breach Involving Personal Information.” See Resources section of this brochure.

California Civil Code section 1798.82-1798.84: Notice of security breach.

C is for Checks.

When accepting payment by check:

DON'T

- Write or enter a credit card number on any documents connected with the transaction.

California Civil Code section 1725: Limitation on collection of personal information when accepting payment by check.

DO

- Verify the consumer’s identity by looking at the driver’s license or other picture ID.
- Verify the consumer’s identity by comparing the signature on the driver’s license with the signature on the check.

C is also for Credit cards.

When accepting payment by credit card:

DON'T

- Write or enter any personal information – home address, driver’s license number, Social Security number, e-mail address, etc. – on any documents connected with the credit card transaction.
- Require individuals to provide personal information as a condition of completing the transaction.

DO

- Verify the consumer’s identity by looking at a driver’s license or California identification card photo.

- | | |
|--|--|
| | |
|--|--|
- Verify the consumer's identity by comparing the signature on the driver's license to the signature on the back of the credit card and on the receipt.
 - Verify the address and zip code of customers paying by credit card over the telephone, through the mail or by e-mail.

California Civil Code section 1747.08: Limits on collection of personal information when accepting payment by credit card.

D is for Destruction of documents.

When destroying customer records containing personal information:

DON'T

- Throw paper records containing personal customer information – home address, account number, Social Security number, driver's license number, etc. – into the trash without first shredding them.
- Dispose of or give away old computers, hard drives, photocopiers or fax machines with hard drives, computer disks, tapes or other electronic media containing personal information without first making the data unreadable.

California Civil Code section 1798.80-1798.81: Destruction of customer records. Also see federal Fair Credit Reporting Act section 628: Disposal of Records.

DO

- Use a cross-cut shredder to destroy paper customer records containing personal information before throwing them away.
- If you use a shredding service, prefer one that shreds the documents on site.
- Use software to over-write computer hard drives containing personal information before disposing of them.
- Destroy disks or tapes containing personal information before disposing of them.

D is for Driver's licenses.

If you “swipe” or scan a driver's license to read the information on the magnetic strip:

DON'T

- Retain or use any of the information for any purpose other than the following:
 - to verify the customer's age or the authenticity of the license;
 - to comply with a legal requirement to record, retain or transmit the information;
 - to transmit the name and identification number to a check service company for approving payments; or
 - to report, investigate or prevent fraud.

California Civil Code section 1798.90.1: Confidentiality of driver's license information.

DO

- Verify a customer's age by looking at the driver's license or California identification card photo and birth date.

I is for Identity theft and debt collection.

DON'T

- Continue to try to collect a debt from someone who provides you with a copy of a police report and other documentation of identity theft.

DO

- Review and consider the police report and other information provided by someone claiming to be an identity theft victim.
- Stop collection activities—and notify credit reporting agencies and the creditor—if you determine that the consumer's debt is the result of identity theft.
- Notify the consumer in writing—before resuming collection activities—if you make a good faith determination that the information does not establish that the consumer is not responsible for the debt.

California Civil Code section 1788.18: Responsibilities of debt collectors in identity theft situations. Also see California Civil Code sections 1798.92-1798.97: Identity theft victim's rights against claimants.

I is for Identity theft and providing documents.

Identity theft victims are entitled to copies of documents on fraudulently opened accounts.

DO

- Give an identity theft victim who requests it copies of applications, telephone or electronic records, and other documents on accounts opened fraudulently in the victim's name.
- First ask the victim to send you a copy of his or her police report of identity theft and other identifying information.

California Penal Code section 530.8: Access to fraudulent account information.

P is for Privacy policy statement.

If you operate a commercial Web site that collects personal information on California residents:

DO

- Say what you do: Post a statement of your privacy policy in a conspicuous location on your Web site.
- Do what you say: Comply with the terms of your privacy policy.
- In your privacy statement, identify the categories of personal information that you collect through the Web site on people who use or visit your site.
- In your privacy statement, describe any process you maintain that allows someone to review or ask for changes to any of his or her personal information collected through the Web site.
- In your privacy statement, describe the process you use to notify those who use or visit your site of changes to your privacy policy.

- In your privacy statement, identify the effective date of the policy.

California Business & Professions Code sections 22575-22579: Online privacy protection act (effective July 1, 2004).

R is for credit card Receipts.

If you electronically print out customer receipts for credit card transactions:

DON'T

- Print more than the last five digits of a credit card number on the receipt given to the customer.

California Civil Code section 1747.09: Truncation of credit card numbers.

R is for Respond to Requests for information-sharing lists.

If you share customer personal information with other companies for direct marketing purposes:

DO

- Respond to a customer who asks which companies you shared customer personal information with in the past year.
 - Give your customer a cost-free opportunity to opt out of, or say no to, sharing their personal information with other companies for marketing purposes.
 - If you don't give your customers the right to opt out of sharing their information for marketing purposes, tell them how to get a list of the types of information shared and the companies with whom it was shared.
- Make your customer information-sharing list available in a variety of ways: for example, on your Web site, at retail locations, through the mail.
- Inform your customer contact staff on how to respond to customer requests for this information.

S is for Security.

If you collect or retain personal information - including sensitive information such as Social Security number, driver's license number, state ID card number, credit card or other financial account number, or medical information - of California residents:

DO

- Use reasonable security measures to protect the personal information from unauthorized access, use, disclosure, modification or destruction.
- Make sure that your contracts with service providers and others with whom you share personal information require those companies to protect the personal information with reasonable security measures.
- Adopt a written information security policy and make sure employees know what is expected of them.
- Security measures include administrative, physical, and technological safeguards.
- Administrative safeguards include the following:
 - Limit access to records containing sensitive personal information to those who need to use them in the performance of their duties.
 - Adopt a "clean desk policy," requiring employees to properly secure records containing sensitive personal information.
- Physical safeguards include the following:
 - Store paper records containing sensitive personal information in locked cabinets.
 - Properly dispose of records containing personal information, such as by shredding them. (See page 6 of this Handbook.)
- Technological safeguards include the following:
 - Use firewall, anti-virus and anti-spyware software to secure your computers and network. Update the software regularly.
 - Protect stored data that includes sensitive personal information by encrypting electronic records, including data on laptops and other portable devices.
- Consult guidelines and industry best practices on information security, such as those listed on page 13 of this Handbook.

California Civil Code section 1798.81.5: Personal information security.

DON'T

- Make it hard for your customers to find out about your specific information-sharing practices.

California Civil Code sections 1798.83-1798.84: Personal information disclosure.

S

is for Social Security numbers.

If you collect or retain Social Security numbers of customers or employees:

DON'T

- Publicly post or display an individual's Social Security number in any manner.
- Print an individual's Social Security number on a card required for access to products or services.
- Require an individual to transmit his or her Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted.
- Require an individual to use his or her Social Security number to access an Internet Web site, unless a password or PIN is also required.
- Print an individual's Social Security number on documents that are mailed to the individual, unless state or federal law requires the number to be on the document to be mailed.
- Print more than the last four digits of an employee's Social Security number on a pay stub or voucher - better yet, use an employee ID number instead.

California Civil Code sections 1798.85-1798.86: Confidentiality of Social Security numbers. California Labor Code section 226: Payment of wages.

DO

- Reduce the collection of Social Security numbers: Don't collect them if you don't need them—then you won't have to protect them.
- Tell individuals when you ask for their Social Security numbers why you need them, what you will use them for, and how you will protect them.
- Control access to Social Security numbers, including allowing access only to employees who need it to perform their duties.
- Consult the California Office of Privacy Protection's "Recommended Practices for Protecting the Confidentiality of Social Security Numbers." See Resources section of this brochure.

- | | |
|--|--|
| | |
|--|--|
- Print an employee ID number - rather than a Social Security number - on employee pay stubs or vouchers.

V is for Verify identity *before* granting credit.

DON'T

- Ignore significant differences between the personal information provided by a consumer applying for credit and the information in his or her credit report.
- Ignore a fraud alert or security alert on an applicant's credit report.

DO

- Make an effort to verify the identity of an applicant before granting credit. For example, you could ask to see a driver's license or California identification card and compare the photo and signature. You might ask to see three pieces of ID, such as a military ID, credit card, health plan card or passport, in addition to a driver's license.
- Take extra steps to verify identity if there is a difference between the personal information the applicant provides and the information in his or her credit report. Look especially at the first and last name, address and Social Security number.
 - For example, notice if the name is significantly different – not “Bill” vs. “William,” but “John” vs. “Catherine.” Ask to see additional pieces of identification.
 - If the residence address in the credit report is a different city or state, you might ask to see a utility bill or other proof of residency.
- Tell customers you're taking these steps to protect them from identity theft.
- Call the phone number given with a fraud alert to verify the applicant's identity. Do this before approving the credit application.
- Check picture ID and signature when accepting payment by credit card or check.

California Civil Code sections 1785.11.1 and 1785.20.3: Verifying identity of credit applicants and verifying identity when fraud alert appears on credit history.

Additional Resources

Privacy and Identity Theft Laws

Links to California and federal privacy and identity theft laws can be found on the California Office of Privacy Protection Web site at www.privacy.ca.gov/lawenforcement/laws.htm.

Some types of business - financial services companies and healthcare, for example - are subject to specific federal laws and regulations on privacy.


- The Gramm-Leach-Bliley Act's Privacy and Safeguards Rules apply to a broad spectrum of financial institutions. For more information, see www.ftc.gov/privacy/privacyinitiatives/glbact.html.
- The Health Insurance Portability and Accountability Act's Privacy and Security Rules apply to health care providers, health plans and health care clearinghouses. For more information, see www.hhs.gov/ocr/hipaa/.

Privacy Best Practices

- "Recommended Practices on Protecting the Confidentiality of Social Security Numbers" and "Recommended Practices on Notification of Security Breach Involving Personal Information" can be found on the California Office of Privacy Protection Web site at www.privacy.ca.gov/recommendations/recomend.htm.
- The widely accepted Fair Information Practice Principles are the basis for many privacy laws in the United States, Canada, Europe and other parts of the world. The Principles were first formulated by the U. S. Department of Health, Education and Welfare in 1973. The principles can be found in the Organization for Economic Cooperation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at www1.oecd.org/publications/e-book/9302011E.PDF.
- *Privacy for Business™: Web Sites and Email*, Stephen Cobb (Dreva Hill, 2002).

Security Best Practices

- Business Security Information, Federal Trade Commission, available at www.ftc.gov/bcp/online/edcams/infosecurity/businfo.html.
- "Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices" (July 2002), Internet Security Alliance, available at www.isalliance.org.

- 
- Payment Card Industry Data Security Standard, available at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf or at <https://sdp.mastercardintl.com/>.
 - “Security Check: Reducing Risks to Your Computer Systems,” Federal Trade Commission, available at www.ftc.gov/bcp/online/pubs/buspubs/security.htm.



Arnold Schwarzenegger
Governor

Rosario Marin
Secretary
State and Consumer Services Agency

Carrie Lopez
Director
Department of Consumer Affairs

Joanne McNabb
Chief
Office of Privacy Protection